



1 / 4

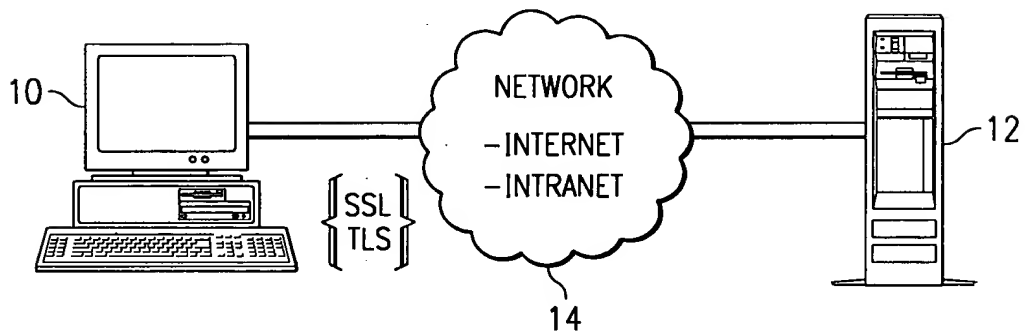


FIG. 1
(PRIOR ART)

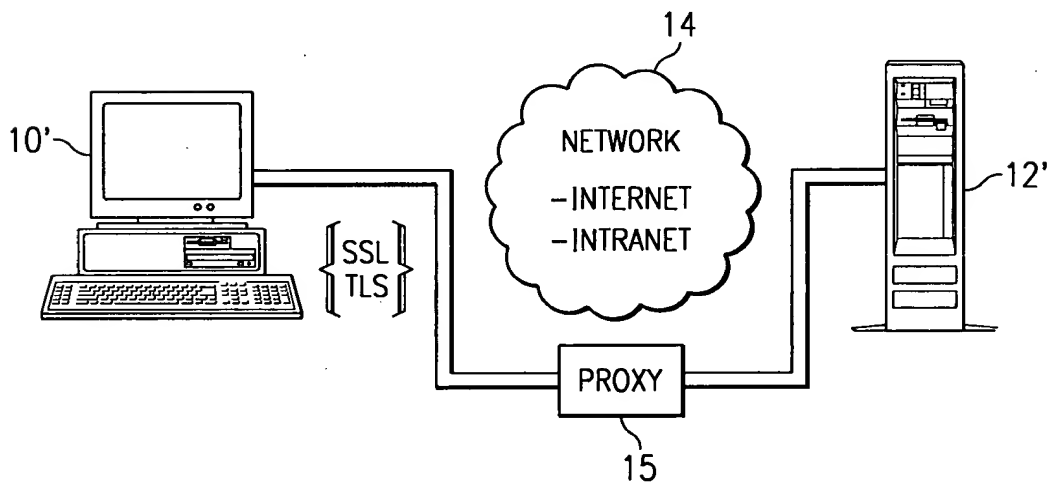


FIG. 2
(PRIOR ART)



2 / 4

FIG. 3A

Client (1)	Proxy (1)	Client (2)	Proxy (2)	Origin Server
ClientHello				
20	ServerHello			
	Certificate*			
	CertificateRequest*			
	ServerKeyExchange*			
Certificate*				
ClientKeyExchange				
CertificateVerify*				
changeCipherSpec				
Finished				
22	changeCipherSpec	24		
	Finished	HTTP "connect"	26	
			Create session ID	
		ClientHello		
			28	ServerHello
				Certificate*
				CertificateRequest*
				ServerKeyExchange*
		Certificate*		
		ClientKeyExchange		
		CertificateVerify*		
		changeCipherSpec	30	
		Finished		
32				
Send "master secret" w/ proxy session ID				changeCipherSpec

TO FIG. 3B



3 / 4

FIG. 3B

FROM FIG. 3A

	Calculate key-block based on "master secret"			Finished
	34	HTTP Request	38	
		36	Update/modify request	40
				HTTP content reply
		42	Transcode reply	
			Send second request	
			44	HTTP content reply
			(2) ClientHello	
				(2) ServerHello
				(2) Certificate*
				(2) CertificateRequest*
				(2) ServerKeyExchange*
			(2) Certificate*	
			(2) ClientKeyExchange	
			(2) CertificateVerify*	
			(2) changeCipherSpec	
			(2) Finished	
				changeCipherSpec
changeCipherSpec	Notify client of cipher spec change		48	Finished
Finished			Send third request	
		50		HTTP content reply
			Transcode final reply	
		Render reply		



4 / 4

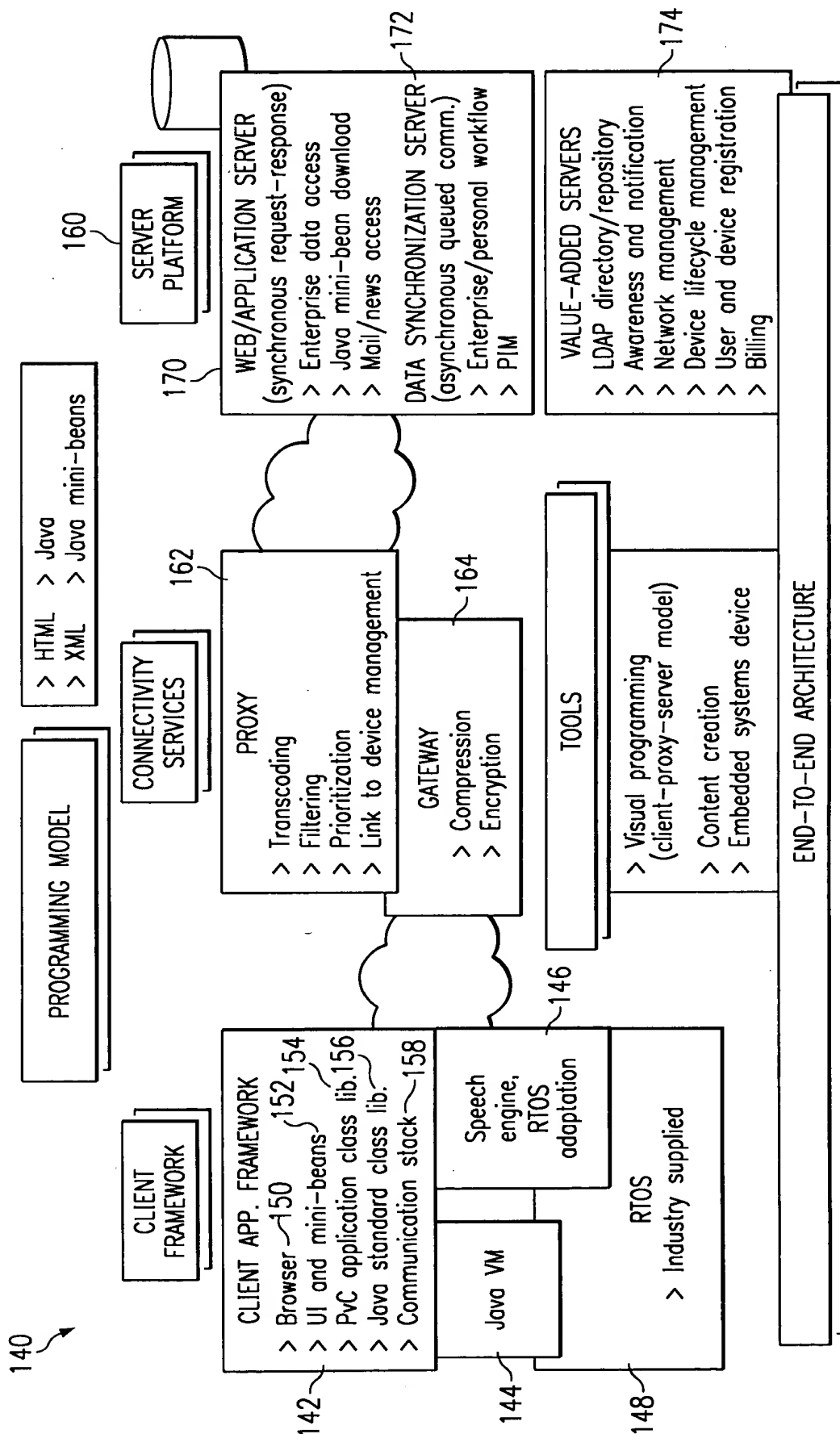


FIG. 4